Abstract

EXTENSION OF X.509 CERTIFICATES TO SIMULTANEOUSLY SUPPORT MULTIPLE CRYPTOGRAPHIC ALGORITHMS

A technique permitting an X.509 certificate to simultaneously support more than one cryptographic algorithm. An alterative public key and alternative signature are provided as extensions in the body of the certificate. These extensions define a second (or more) cryptographic algorithm which may be utilized to verify the certificate. These are not authenticated by the primary signature and signature algorithm in the primary cryptographic algorithm. These newly defined extensions are reviewed by a receiving entity if the entity does not support the cryptographic algorithm of the primary signature.